Automatic Decryption of Images through Artificial Neural Networks

Hüsamettin UYSAL
Department of Electronics and Communication Engineering
Yildiz Technical University, YTU
Istanbul, Turkey
husamettin.uysal@bilecik.edu.tr

Sinem KURT
Department of Electronics and Communication Engineering
Yildiz Technical University, YTU
Istanbul, Turkey
sinem.kurt@bilecik.edu.tr

Tülay YILDIRIM
Department of Electronics and Communication Engineering
Yildiz Technical University, YTU
Istanbul, Turkey
tulay@yildiz.edu.tr

***Abstract*—In recent days, it has become important to ensure the security of digital images. For this reason, a variety of encryption and decryption methods have been produced. Therefore the encryption methods increasing day by day frequently cause to change the codes of encrypted digital images. This causes the users to update their codes. This system tries to decrypt automatically using Artificial Neural Network (ANN) without knowing what the decoder. In this study, decryption through MLP (Multilayer Perceptron) and RBF (Radial Basis Function) networks was tested using the interface which was designed in Matlab GUI and the image was shown and saved with minimum error by calculating the error rates of decrypted images.**

Keywords-component; image encryption; image decryption; neural network

I. INTRODUCTION

Cryptology is a compound of the Greek words crypto's (hidden) and lo'gos (word) and is assessed as the science of secrecy-confidentiality in communication. In commercial relations, state affairs, military affairs and personnel affinities, the reliable conduct of business activities is a major concern.

It is necessary to ensure that the data is transferred safely in inter-system connections or correspondence between two points. This is ensured by encrypting the outgoing data. Thus, the reliable transmission of the data is ensured using open communication channels. If a correspondence channel is utilized for communications, the assumption that the confidential information may be heard by an authorized person or this person may infiltrate (intervene) the communication channel to corrupt or alter (sending faulty data) the data has always been a significant concern.

Cryptology is essentially divided into two mains: Cryptography (encryption) and cryptanalytic (decryption). The original communication that shall be sent is called plain text while the encrypted form of this test is referred to as cipher text-cryptograph.

Encryption has been used in military and diplomatic communication (correspondence) for a thousand years to ensure the security of data. However, it is not needed by the private sector as well. The communications between computers regarding financial transactions (e.g.: credit rates) are conducted using open channels. While using these open channels, cryptology is necessary to ensure the aforementioned transactions are conducted safely and confidentially [1].

In this work, the images are encrypted with an encryption function on Artificial Neural Network (ANN) and that images are decrypted automatically using ANN in order to attain the initial image. The encryption function is shown Equation 1. The RBF (Radial Basis Function) and MLP (Multilayer Perceptron) network structures are utilized for this competition and the differences of two networks are observed.

The projects related image cryptology is shown in the following studies. Bhowmik and Acharyya studied on image security using a combination of block-based image transformation and encryption techniques with genetic algorithm [4]. Enayatifar and Abdullah studied on a method based on a hybrid model composed of a genetic algorithm and a chaotic function for image encryption [2]. Gupta and Jain studied on implementation of securely using steganographic technique using genetic algorithm and visual cryptography using pseudorandom number [3]. However there is not any study which uses artificial neural network in competition of both encryption and decryption.

II. IMAGE ENCRYPTION PROCESS

Cryptography is the science of converting information in readable format into another format that others cannot read, i.e. the science that deals with the security of information. Considering the dazzling speed of today's technology, the security gap posed by the developing

technologies gains significance. In today's world of computers, the image security has become an important issue. Encryption is used to ensure this security. Cryptology is the science of encryption. Encryption is used to encrypt various communications, texts and images and sending these messages to the receiver through secured media. We, in consideration of this, decided to encrypt images. Image encryption has various fields of application. It is particularly important for the protection of military positioning diagrams, banks' structural blueprints and data received from the military satellites. Three simple types of encryption equipment exist;

- Self-operated encryption modules
- Encryption boxes dedicated to communication connections
- Cards plugged into personal computers

The self-operated encryption modules are typically used for password confirmation and key management by banks and similar organizations.

The dedicated encryption boxes are generally used to secure the point-to-point information transfer between two sites.

The card encoders used in personal computers normally encrypt all data sent to the hard-disk and may be configured to encrypt data sent to other storage units such as disk drivers.

A. Image Encryption Methods and Algorithms

The use of different secured communication media, in addition to the data encryption methods existing today, has become a necessity. One of these secure communication media is image data encryption. Below are the most common forms of today's image encryption methods.

1) Image encryption through digital signature

Digital signature comprises of a series of characters attained using the hidden key of the signed text and the signer. Digital signature is a method attempting to provide the same properties of handwritten signature with the electronic documents as well. Thanks to the encryption methods, it is only possible to determine from an electronically signed document that it was issued by the signer which assures that the document's integrity is preserved. It is very difficult to copy a digital signature; furthermore, the source of the digital signature, i.e. the person that appended the signature can be proven without raising doubt [5].

2) Encryption using SCAN language

This is a method that provides lossless encryption in binary and grey image types. The encryption scheme is based on the SCAN patterns arising from the SCAN method. SCAN is a rapid, figural language based, two-dimensional access approach using several scanned path patterns.

Through this method, any binary image is encrypted by specifying a scan path coded on the image and coding the bit array of this path. An image encrypted using an encryption method cannot be deciphered as long as the encryption algorithms are kept secret. However, the algorithms for most of the encryption methods are well known. The existing encryption algorithms depend on a hidden key rather than the secrecy of the encryption algorithm [5].

3) Mirror-like image encryption algorithm

This is an image encryption algorithm based on complex image encryption method. Depending on a binary array produced from a complex system, the image pixels are scrambled. Since a parallel process is applied, it has properties like high security and corruption avoidance. This method is an image encryption algorithm with translocation feature [5].

4) Complex image encryption algorithm

This is an image encryption system based producing a complex array. Each binary array produced is reused. The image's pixels are reorganized as per the binary array. This is based on a scan model and the image is reformed according to this scan model [5].

5) BRIE image encryption algorithm

While this is a new image encryption algorithm, it uses the complex image encryption system. It is defined by a function using bit scrolling from a complex system and a binary array, and each pixel on the image is converted into a grey image pixel. This system is cost effective due to the application of its structure and its architectural structure while also an easy method thanks to its high calculation speeds. Consequently, when two encrypted images are simulated, the size of the original image is compared with the encrypted image's calculated size, it is seen that this algorithm has a very effective structure. This algorithm is comprised of three fundamental notions;

- Value conversion
- Position permutation
- The combinations of these

The value conversion is the new value of the original signal's data value after going through the process in the algorithm. Position permutation algorithms allows the original data positions to permutate (translocate). Consequently, the combination form permutations combine together the position permutation and value conversion [10].

In this study, the three-dimensional image used is initially set through Gray Scale conversion to attain a two-dimensional image. After that, the two-dimensional image is converted to one-dimensional array. The new value is got putting in place 'x' in the function at Equation 1 for each value of the one-dimensional array. Thus, the outputs which are attained are pixel value of the encrypted image. The encrypted image is shown on the screen converting from one-dimensional array to two-dimensional image. After all, the encryption process is completed. The reason of using the function which is identified as equation 1 instead of using

one of the methods which is mentioned above is given precedence competition of decryption using artificial neural network in this project.

Secondly, the outputs are got putting in the function the all value between 0-255 before decryption competition and the network is trained with this output and input value. The input value is 'y' and the output value is 'x' in the function. Thus, the network gives the pixel value of the original image when the pixel value of the encrypted image is applied it.

Finally, the original image is attained again through artificial neural network.

The function which we use to encode images is as follows;

$$y_1k = \mathrm{I}(x\mathrm{I}\uparrow 10\,\mathrm{I}\,3\,\mathrm{I}\,x + 128) + (100\,\mathrm{I}\,(\mathrm{I}(11)\mathrm{I}\uparrow t) \quad (1)$$

- x: Normalized value of the image pixel
- t: Original value of the image pixel
- y_k: The pixel value of encrypted image

III. RBF Based Artificial Neural Networks

The artificial neural networks are the result of the activity to form the mathematical model of the learning process, inspired by the human brain. The Artificial Neural Networks (ANN), are capable of learning and generalizing through trial [6].

The artificial neural networks (ANN) are computer systems developed to automatically perform abilities like forming and discovering new information through learning, a feature of the human brain, without any assistance. Figure.1 shows a multi-layer artificial neural network where several neurons are interconnected. The layer(s) between the input layer and the output layer are called hidden layers. The number of layers that shall be used in neural networks or the number of neurons in each hidden layer has not yet been defined; these problem-variable features are determined through trial and error [7].

RBF is a different approach propounding the curve fitting in multidimensional space problem. Learning equals to statistically detecting the surface that is most suitable for the training data in the multidimensional space. RBF network is comprised of input and output layers as well as one hidden layer. While the conversion from the input space to the hidden layer space is non-linear, the transference from the hidden layer to the output space is linear [9].

The working principle of a RBF network can be explained as setting the RBFs with hidden layers into the solution space with the appropriate width and central parameters to attain the desired input-output correlation. This means for input data in the data set, each RBF on the network produces a value that has a direct proportion to the distance with its center. The value produced by RBFs is weighted and added. Therefore, the output produced by the network for the input data is attained. While conducting clustered operations or with limited time or space, it is advantageous to adjust at the beginning the processors within the hidden layer of the neural to allow for the desired cluster. Therefore, the use of processors with a specific area of effect is preferred over the constantly increasing processors. These processors may take the form of triangle, trapezoid, semicircle and similar shapes and are more suitable for theoretical and practical calculations in mathematics as their derivative can be calculated. Therefore, a Gaussian shaped processor is usually the choice [5,6]. The Gauss function, selected as the activation function for RBF is defined as follows;

(2

X defines the input vector, while u_j and s_j define the radial basis function G's and width parameter's center value of j. hidden neuron. The term $\|\cdot\|$ refers to the Euclid distance. In RBF model, the network's output value is calculated as follows;

$$y_k = \sum_{j=1}^{P} W_{jk} a_j + W_o \quad (3)$$

W_{jk}; is the weight between j. hidden neuron and k. output neuron, while W_0 is the bias factor and P is the number of hidden neurons [10].

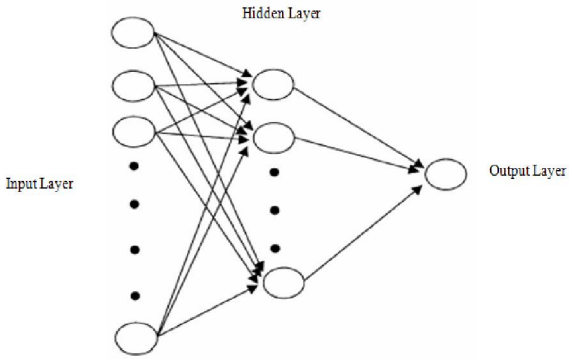

Figure 1. Feed-forward multilayer artificial neural network

In this study, the spread constant is determined as 0.08.

IV. MLP Based Artificial Neural Networks

The multilayer perceptron consists of a system of simple interconnected neurons, or nodes, as illustrated in Fig. 2, which is a model representing a nonlinear mapping between an input vector and an output vector. The nodes are connected by weights and output signals which are a function of the sum of the inputs to the node modified by a simple nonlinear transfer, or activation, function. It is the

superposition of many simple nonlinear transfer functions that enables the multilayer perceptron to approximate extremely non-linear functions. If the transfer function was linear then the multilayer perceptron would only be able to model linear functions.

Due to its easily computed derivative a commonly used transfer function is the logistic function. The output of a node is scaled by the connecting weight and fed forward to be an input to the nodes in the next layer of the network. This implies a direction of information processing; hence the multilayer perceptron is known as a feed-forward neural network. The architecture of a multilayer perceptron is variable but in general will consist of several layers of neurons. The input layer plays no computational role but merely serves to pass the input vector to the network. The terms input and output vectors refer to the inputs and outputs of the multilayer perceptron and can be represented as single vectors, as shown in Fig. 2. A multilayer perceptron may have one or more hidden layers and finally an output layer. Multilayer perceptron are described as being fully connected, with each node connected to every node in the next and previous layer [11].

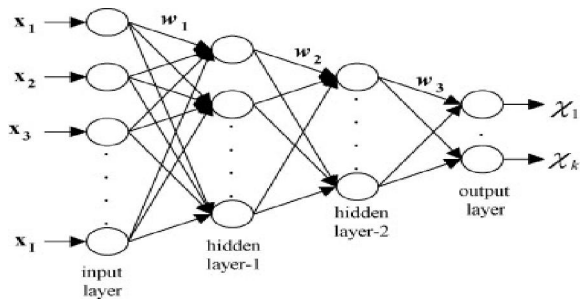

Figure 2. Multilayer perceptron with two hidden layers

In this study, a 3-hidden layer-MLP network with the tangent hyperbolic function as activation function is used. The quasi-newton backpropagation algorithm is used as training algorithm. The neuron numbers are selected as 8,4,8 for the hidden layers, respectively.

V. THE PROJECT IMPLEMENTATION AND THE RESULTS

The interface which is designed in Matlab GUI is shown in the following, Figure 3.

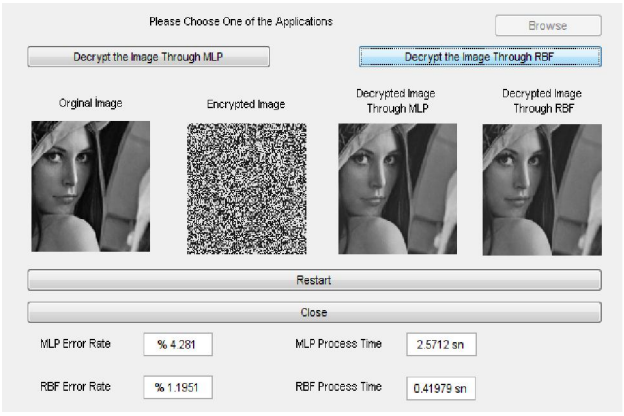

Figure 3. The Interface which is designed in Matlab GUI

Original image, encrypted image, decrypted image with MLP, decrypted image with RBF are seen above (from left to right). The error rates and processing time of decrypted images with MLP and RBF have been written on the screen. The image which has minimum error rate has been shown and saved.

The decrypted image with MLP has 4.281% error rate and the same decrypted image with RBF has 1.1951% error rate. MLP processed this in 2.5712 seconds and RBF processed it in 0.41979 seconds.

The some practices made with this study are shown in Figure 4.

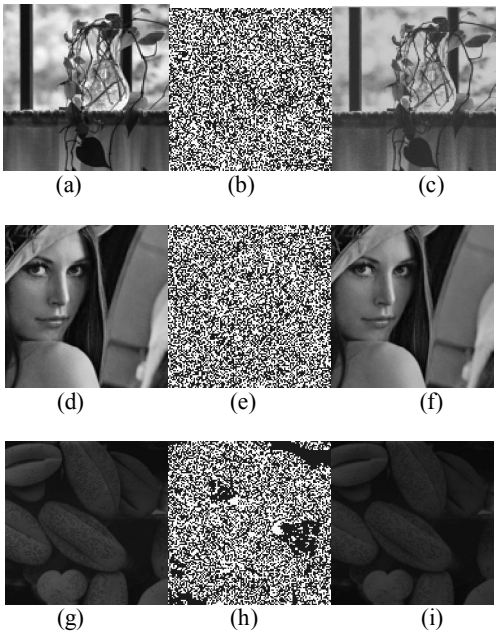

Figure 4. (a), (d), (g) original images; (b), (e), (h), encrypted images; (c), (f), (i) decrypted images.

VI. CONCLUSION

Cryptography is used in transmitting images in a safe way. The cryptograph process occurs by applying the

inverse of the same encoding method used, for decoding on the transmitting side. Nowadays, in the light of continuous update in encoding methods, the process becomes quite slow and difficult to apply. In this study, it is aimed to update code automatically using Artificial Neural Network (ANN) and decode without any additional computation on the transmitted side. Also, the differences between RBF and MLP have been determined in this study. RBF was better than MLP with shorter processing time and less error rate. The main difference of this study from other related ones is using ANN for encoding and decoding. The procedure of this study consists of decoding the encrypted images by ANN to obtaining the original image. As a result, it is succeeded to obtain almost the same image of the original image easily by ANN.

REFERENCES

[1] Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software, 22 August 2000.

[2] Rasul Enayatifar, Abdul Hanan Abdullah, "Image Security via Genetic Algorithm", International Conference on Computer and Software Modeling IPCSIT vol.14, 2011

[3] Ravindra Gupta, Akanksha Jain, "Integrating Steganography Using Genetic Algorithm and Visual Cryptography for Robust Encryption in Computer Forensics", International Journal of Electronics and Computer Science Engineering, 2012

[4] Sandeep Bhowmik, Sriyankar Acharyya, "Image Cryptography: The Genetic Algorithm Approach", Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference

[5] Güvenoğlu E., "Görüntü Şifrele Algoritmaları ve Performans Analizleri", Yüksek Lisans Tezi, 2006

[6] J.Park,I.W. Sandberg, Universal Approximation Using Radial Basis Function Networks, Neural Computation, Cilt 3, 246- 257, 1991.

[7] J.Park,I.W. Sandberg, Approximation and Radial Basis Function Networks. Neural Comput., 1993, 5, 305–316.

[8] H.Demuth, M. Beale, Neural Network Toolbox For Use with MATLAB User's GUIde Version 4, MA, 2000.

[9] P.Venkatesan, S.Anitha, Application Of A Radial Basis Function Neural Network For Diagnosis Of Diabetes Mellitus Current Science, Vol. 91, NO. 9, 10 november 2006.

[10] S.R Dorling and M.W Gardner, Artificial neuralnetworks (the multilayerperceptron) —a review of applications in the atmospheric sciences. Volume 32, Issues 14–15, 1 August 1998, Pages 2627–2636.